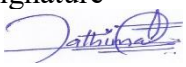
MES COLLEGE OF ENGINEERING, KUTTIPPURAM
DEPARTMENT OF COMPUTER APPLICATIONS
20MCA245 – MINI PROJECT

PRO FORMA FOR THE APPROVAL OF THE THIRD SEMESTER MINI PROJECT

(Note: All entries of the pro forma for approval should be filled up with appropriate and complete information.Incomplete Pro forma of approval in any respect will be rejected.)

Mini Project Proposal No : 1 *(Filled by the Department)*	Academic Year : 2020-2022 Year of Admission : 2020

1. Title of the Project : Detecting DDoS Attack Using Hybrid Machine Learning Algirithms
2. Name of the Guide : Dr. Geevar C Zacharias
3. Number of the Student : 1
4. Student Details (in BLOCK LETTERS)

Name	Roll Number	Signature
1. FATHIMATH SUHARA M A	18	

Date:

Approval Status : Approved / Not Approved

Signature of
Committee Members :

Comments of The Mini Project Guide Dated Signature

Initial Submission :

First Review :

Second Review :

Comments of The Project Coordinator Dated Signature

Initial Submission :

First Review

Second Review

Final Comments :

Dated Signature of HOD

DETECTING DDoS ATTACK USING HYBRID MACHINE LEARNING ALGORITHMS

18-Fathimath Suhara M A

Introduction:

Security has become a necessity with the development of the Internet and networking technology. It is a set of rules and configurations considered to protect network from various security attacks. Most of the security mechanisms must provide the following security services [1].

A. Confidentiality : Protecting data from unauthorized users.

B. Availability : Ensures the data is available to legitimate users at all times

C. Integrity : Ensures that data cannot be altered or duplicated or replayed during transmission

D. Non-Repudiation : Ensures that user does not refuse that he has used the network.

E. Access Control : Controlling the access of unauthorized use of resources.

F. Authentication : Authentication means that the identity of the user is certain

Intrusion is an action that negotiates the three security requirements: Confidentiality, Availability and Integrity of the resources. Intrusion Detection system is an application that inspects network systems for any intrusions. Any suspicious activity will be reported to the administrator or centrally controlled security information and event management system. Whenever a suspicious activity is detected, it issues alerts. IDS's are used to detect various security attacks. [1].

Security Attacks classification [2]

Attack is an indication of security compromise. Security attacks are classified as:

A. Viruses

A virus is a self-copying program that affects and spreads through files. Usually it affixes itself to the files, which will cause it to be run when the file is launched. There are several types of viruses such as, Macro Viruses, System and Boot Record Infectors, File Infectors.

B. Worms

These are self-reproducible programs that spread through the network. They do not need an infected file to circulate. Worms are of two types: mass-mailing worms and network aware worms.

C. Trojans

A Trojan gives off an impression of being evil, yet for the most part have some dangerous reason. Trojans hold some payload, for example, viruses, information obliteration and remote access strategies.

D. Logic Bombs

Logic bomb is a different form of Trojan that releases its payload when some condition is met.

E. Buffer overflows

Buffer overflows make use of wrong programming methods in which buffers are allowed to be overloaded. The data filling in the buffer which is filled beyond its capacity can overflow into the neighboring memory, then it can either control information or it is utilized to change the program execution. Buffer overflows are of two types of. Heap Buffer Overflows, Stack Buffer Overflow

F. Denial of Service Attacks

These attacks usually interrupt the network service or a system, so that it cannot be used further and to degrade the performance.

Objectives:

With the increase in usage of networking technology and the Internet, Intrusion detection becomes important and challenging security problem. A number of techniques came into existence to detect the intrusions on the basis of machine learning and deep learning procedures. This paper will give inspiration to the use of ML and DL systems to IP traffic and gives a concise depiction of every one of the ML and DL strategies. This paper gives an audit of 40 noteworthy works that covers the period from 2015 to 2019. ML and DL methods are compared with regard to their accuracy and detection potential to detect different types of intrusions. Future Research includes ML and DL methods to find the intrusions so as to improve the detection rate, accuracy and to minimize the false positive rate.

Problem Definition:

A review has been made of the significant works in the fields of machine learning and deep learning that are used to detect NIDS and or HIDS during the period of 2015 to 2019. All these woks have emphasized distinct machine learning and deep learning strategies utilized, informational index or datasets utilized, assessment measurements for every one of the systems utilized. To decide the powerful approach a few criteria must be considered. The criterion included classification time, training time, detection rate and accuracy. It is hard to distinguish a superior methodology of ML and DL strategies dependent on just one factor like accuracy.

Basic functionalities:

Tools / Platform, Hardware and Software Requirements:

Hardware specification:The selection of hardware is very important in the existence and proper working of any software. Then selection hardware, the size and capacity requirements are also important.

- Processor : Intel Pentium Core i3 and above
- Primary Memory : 4 GB RAM and above
- Storage : 500 GB hard disk and above
- Display : VGA Colour Monitor
- Key Board : Windows compatible
- Mouse : Windows compatible

Software specification: One of the most difficult tasks is selecting software for the system, once the system requirements is found out then we have to determine whether a particular software package fits for those system requirements. The application requirement:

- Front end : Python Django
- Back end : MYSQL
- Operating system : windows 7 and above
- IDE : PyCharm, Android Studio
- Others : HTML,CSS